CSA cloud security alliance

Cloud Security “Assumption Busters”

CSA initiatives for payoffs and protection

Ron Knode (CSC)

rknode@csc.com

The “big rocks” of cloud security assumptions *…Take care of the big rocks first …*

❶ I must yield to the “genesis syndrome” and start my cloud security journey from scratch

- *“No one really understands my cloud security needs!”*

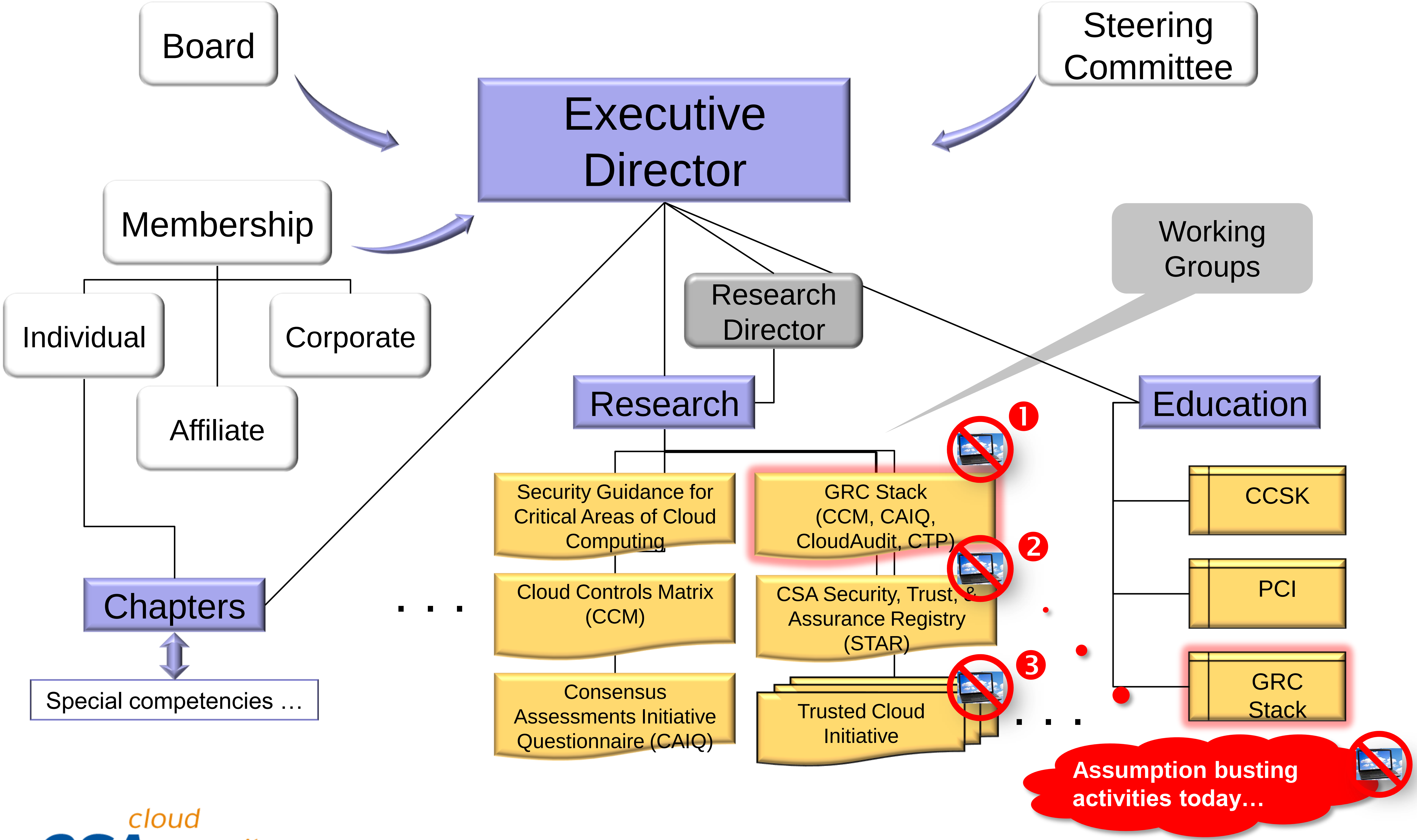
❷ I can never know all the security claims and capabilities and compliance status for all the cloud service offerings available to me

- *“There are too many alternatives and I don’t know all the questions to ask (or answer)!”*

❸ There is no template I can use to put all the necessary pieces together to create (or buy) a cloud service that is trusted enough for me

- *“I will never have the time or horsepower to go through all the steps or check all the circumstances of security for my cloud needs!”*

CSA "Assumption Busting" Organization & Operation & Busting Actions



Board

Steering Committee

Executive Director

Membership

Individual

Corporate

Affiliate

Chapters

Special competencies …

Research Director

Working Groups

Research

Education

Security Guidance for Critical Areas of Cloud Computing

Cloud Controls Matrix (CCM)

Consensus Assessments Initiative Questionnaire (CAIQ)

GRC Stack (CCM, CAIQ, CloudAudit, CTP)

CSA Security, Trust, & Assurance Registry (STAR)

Trusted Cloud Initiative

CCSK

PCI

GRC Stack

1

2

3

Assumption busting activities today…

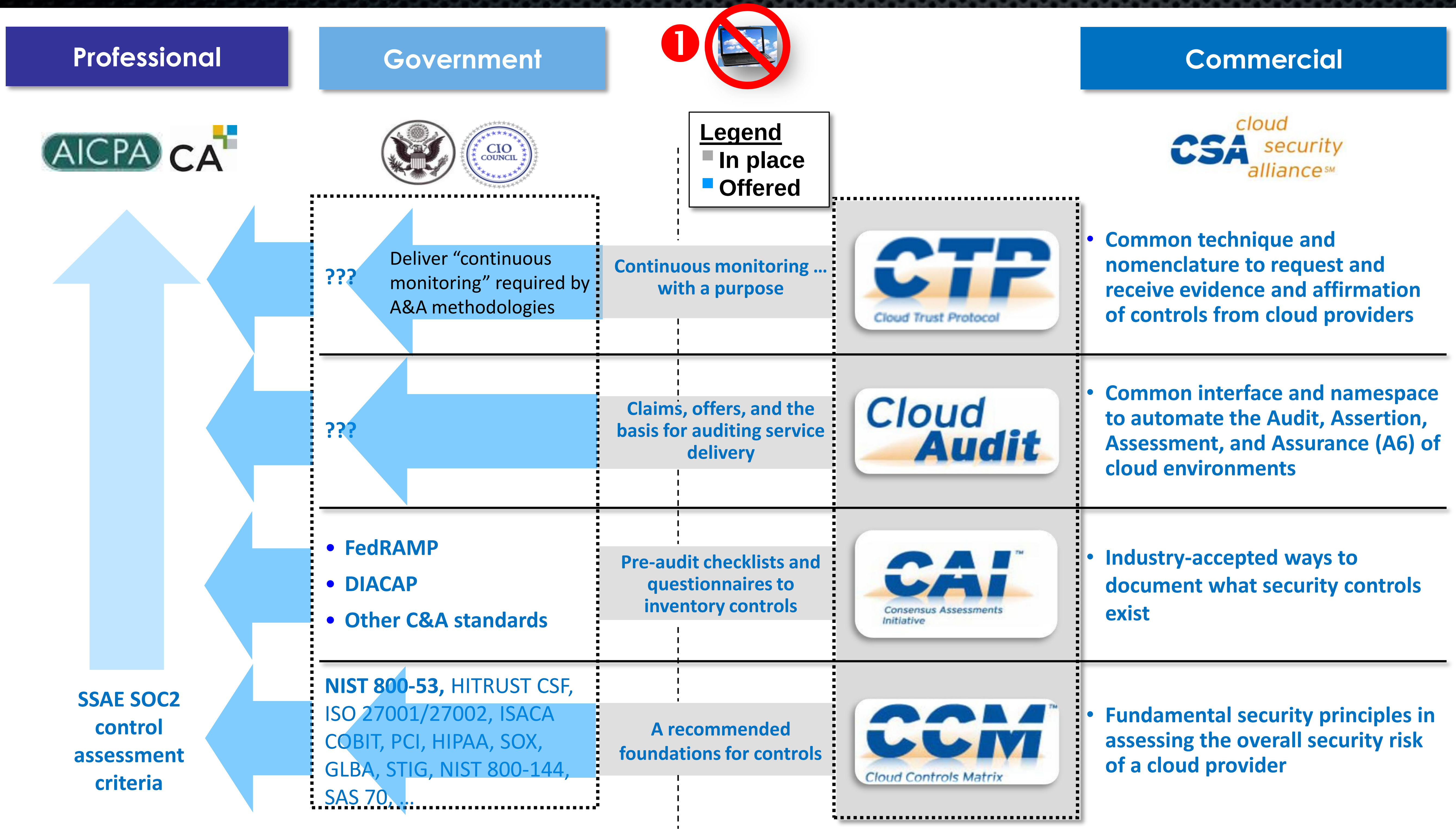
www.cloudsecurityalliance.org

A Complete Cloud Security Governance, Risk, and Compliance (GRC) Stack

❶

Delivering	← Stack Pack →	Description
Continuous monitoring … with a purpose	CTP Cloud Trust Protocol	• Common technique and nomenclature to request and receive evidence and affirmation of current cloud service operating circumstances from cloud providers
Claims, offers, and the basis for auditing service delivery	Cloud Audit	• Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments
Pre-audit checklists and questionnaires to inventory controls	CAI™ Consensus Assessments Initiative	• Industry-accepted ways to document what security controls exist
The recommended foundations for controls	CCM™ Cloud Controls Matrix	• Fundamental security principles in specifying the overall security needs of a cloud consumers and assessing the overall security risk of a cloud provider

A Headstart for Control and Compliance
Forged by the Global Marketplace; Ready for All



Professional | **Government** | **Commercial**

AICPA CA | CIO COUNCIL | CSA cloud security alliance℠

Legend
■ **In place**
🟦 **Offered**

??? Deliver “continuous monitoring” required by A&A methodologies

Continuous monitoring … with a purpose

CTP Cloud Trust Protocol

- Common technique and nomenclature to request and receive evidence and affirmation of controls from cloud providers

???

Claims, offers, and the basis for auditing service delivery

Cloud Audit

- Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments

- FedRAMP
- DIACAP
- Other C&A standards

Pre-audit checklists and questionnaires to inventory controls

CAI™ Consensus Assessments Initiative

- Industry-accepted ways to document what security controls exist

SSAE SOC2 control assessment criteria

NIST 800-53, HITRUST CSF, ISO 27001/27002, ISACA COBIT, PCI, HIPAA, SOX, GLBA, STIG, NIST 800-144, SAS 70, …

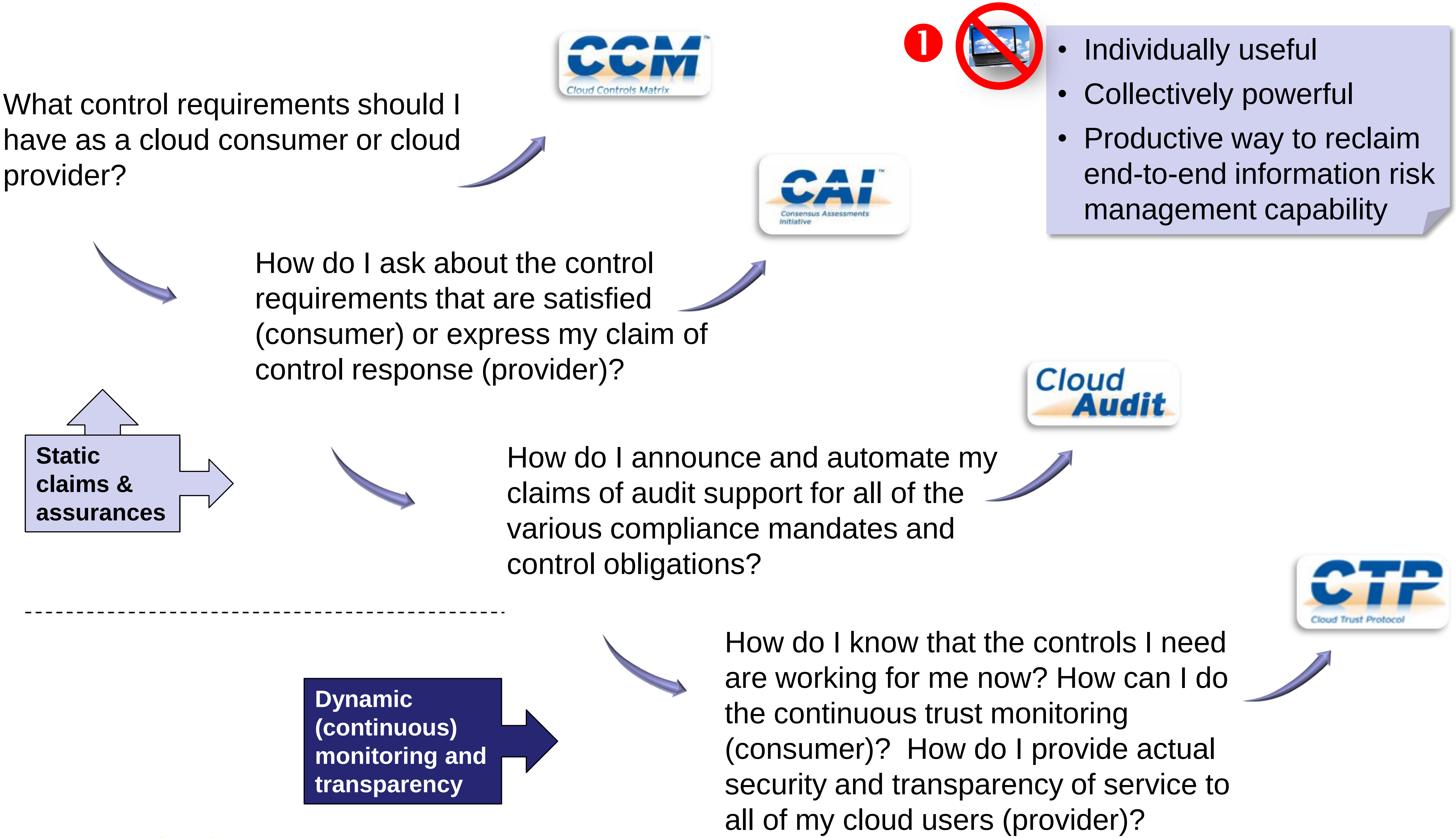
A recommended foundations for controls

CCM™ Cloud Controls Matrix

- Fundamental security principles in assessing the overall security risk of a cloud provider

CSA cloud security alliance

CSA GRC Value Equation for Consumers and Providers



- Individually useful
- Collectively powerful
- Productive way to reclaim end-to-end information risk management capability

What control requirements should I have as a cloud consumer or cloud provider?

How do I ask about the control requirements that are satisfied (consumer) or express my claim of control response (provider)?

Static claims & assurances

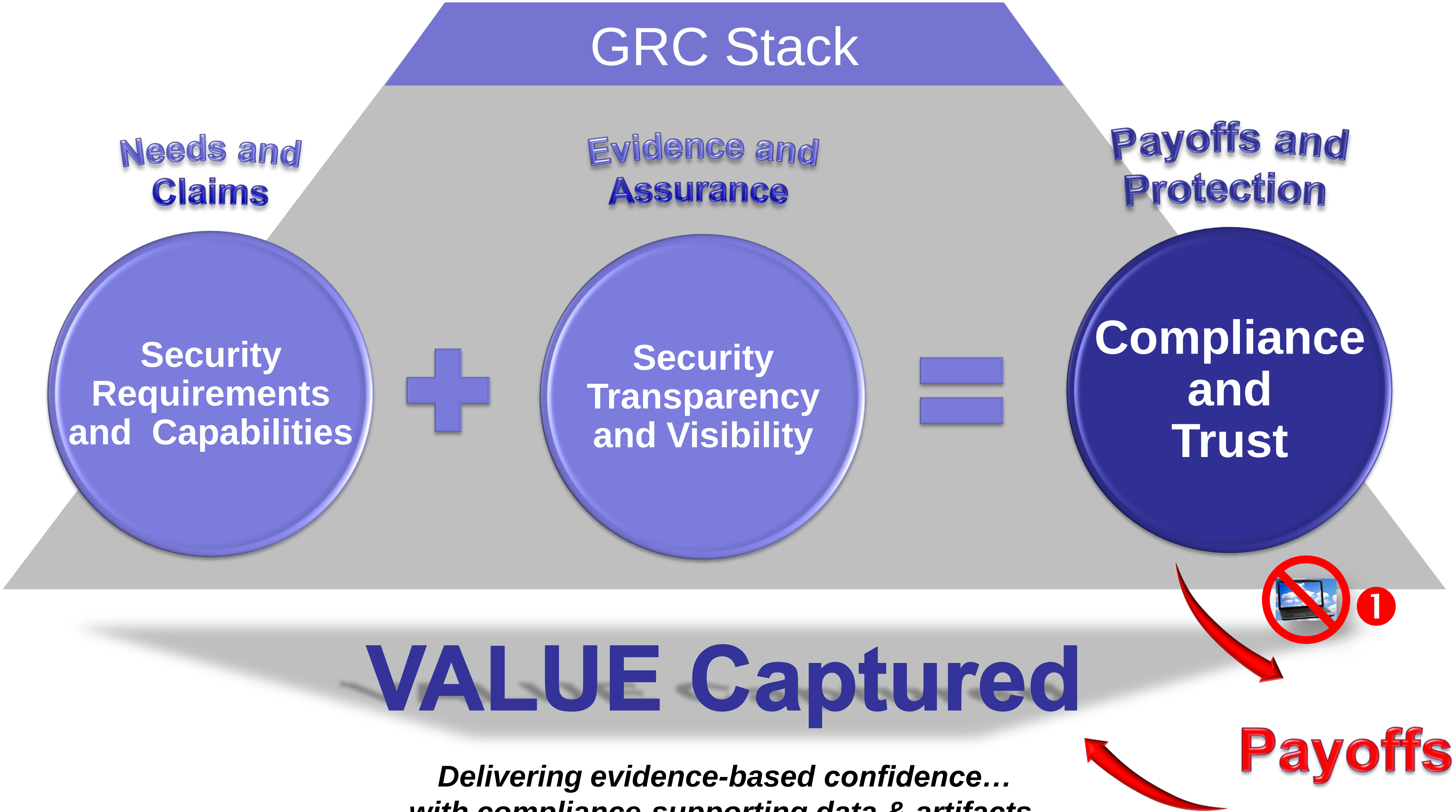
How do I announce and automate my claims of audit support for all of the various compliance mandates and control obligations?

Dynamic (continuous) monitoring and transparency

How do I know that the controls I need are working for me now? How can I do the continuous trust monitoring (consumer)? How do I provide actual security and transparency of service to all of my cloud users (provider)?

The GRC Stack

Solving the Value Equation in the Cloud



GRC Stack

Needs and Claims

Evidence and Assurance

Payoffs and Protection

Security Requirements and Capabilities

+

Security Transparency and Visibility

=

Compliance and Trust

❶

VALUE Captured

Payoffs

Delivering evidence-based confidence…
with compliance-supporting data & artifacts.

GRC Stack Pack Combinations that Deliver a Payoff

❶

GRC Stack Payoff Combinations					Other CSA Related	
CCM Cloud Controls Matrix	CAI Consensus Assessments Initiative	Cloud Audit	CTP Cloud Trust Protocol		CSA STAR Security, Trust & Assurance Registry	TCI
CCM Cloud Controls Matrix	CAI Consensus Assessments Initiative	Cloud Audit			CSA STAR Security, Trust & Assurance Registry	TCI
CCM Cloud Controls Matrix	CAI Consensus Assessments Initiative				CSA STAR Security, Trust & Assurance Registry	TCI
CCM Cloud Controls Matrix		Cloud Audit	CTP Cloud Trust Protocol		CSA STAR Security, Trust & Assurance Registry	TCI
CCM Cloud Controls Matrix		Cloud Audit			CSA STAR Security, Trust & Assurance Registry	TCI
			CTP Cloud Trust Protocol			TCI
CCM Cloud Controls Matrix						TCI

Security, Trust, and Assurance Registry (CSA STAR)

❷

CSA STAR

Security, Trust & Assurance Registry

- Encourage transparency of security practices within cloud providers
- Documents the security controls provided by various cloud computing offerings
- Free and open to all cloud providers
- Option to use data/report based on CCM or the CAIQ

https://www.cloudsecurityalliance.org/star/

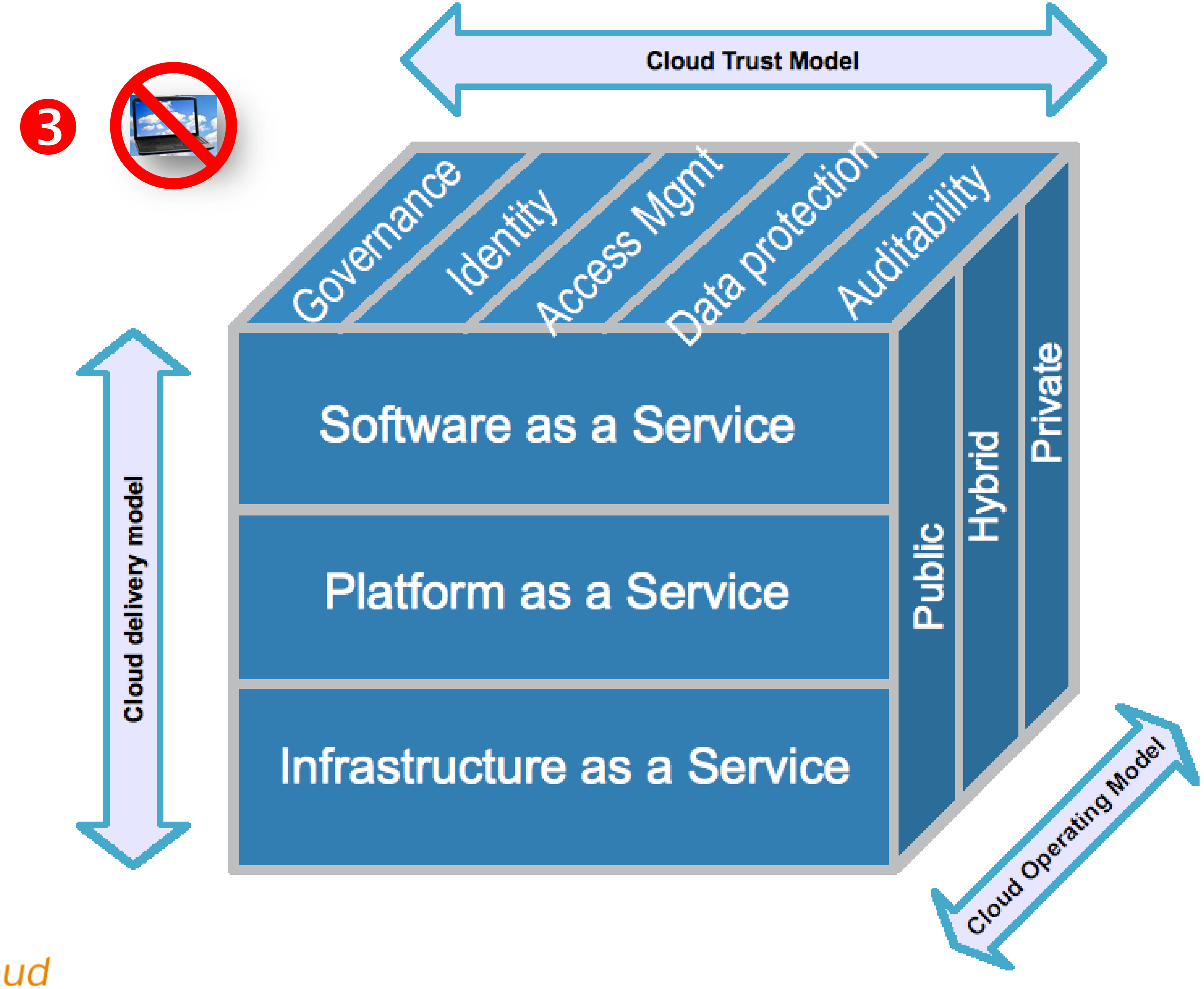
Trusted Cloud Initiative (TCI)

❸

- CSA certification criteria and seal program for cloud providers
- Initial focus on secure & interoperable identity in the cloud, and its alignment with data encryption
- Assemble with existing standards
- Reference models & Proof of concept
- Outline responsibilities for Identity Providers, Enterprises, Cloud Providers, Consumers
- www.cloudsecurityalliance.org/trustedcloud.html

TCI Mission

“To create a Trusted Cloud reference architecture for cloud use cases that leverage cloud delivery models (SaaS, PaaS, IaaS) in the context of operational models (Public, Private, Hybrid) to deliver a secure and trusted cloud service”



What’s Happening Now?

More cloud security “assumption busting” activities

Research Work Groups Underway

- CCM update
- CAIQ update
- CloudAudit update
- CloudTrust Protocol update and integration into CSA GRC stack
- Trusted Cloud Initiative
- CloudSIRT
- Cloud data governance
- Cloud metrics
- Security as a service (SecaaS)

Education

- CCSK update
- GRC stack training
- PCI compliance in the cloud